

PERFORMANCE WORK STATEMENT

FOR

**Support to the Director, Threat Emulation Forces for
Network Integration Evaluation 17.2**

Period of Performance is from 5JUL17 – 9AUG17

Training and Doctrine Command Deputy Chief of Staff for Intelligence

As of 30 March 2017

TABLE OF CONTENTS

SECTION C-1	GENERAL
SECTION C-2	ACRONYMS
SECTION C-3	GOVERNMENT FURNISHED PROPERTY AND SERVICES
SECTION C-4	CONTRACTOR FURNISHED PROPERTY AND SERVICES
SECTION C-5	SERVICES REQUIRED
SECTION C-6	PROGRAM MANAGEMENT SUPPORT
SECTION C-7	DELIVERY, INSPECTION/ACCEPTANCE BY GOVT
SECTION C-8	TECHNICAL EXHIBITS
SECTION C-9	CONTRACT DATA REQUIREMENTS LIST (CDRLs)
SECTION C -10	ATTACHMENTS AND FORMS
ATTACHMENT A	NON-DISCLOSURE AGREEMENT FOR CONTRACTORS
ATTACHMENT B	SENSITIVE DATA NON-DISCLOSURE AGREEMENT
ATTACHMENT C	TRAVEL AUTHORIZATION REQUEST FORM
ATTACHMENT D	CUSTOMER FEEDBACK FORM
ATTACHMENT E	PERFORMANCE REQUIREMENTS SUMMARY (PRS)

C-1 GENERAL

1.0 Background. The U.S. Army Training and Doctrine Command (TRADOC)'s Deputy Chief of Staff for Intelligence (G-2) studies, designs, coordinates, and applies the current and future Operational Environment (OE) input in support of Joint and Army programs for training and leader development, concept development, experimentation, and requirements determination. To accomplish this mission and core function, TRADOC G-2's Threat Emulation Force (TEFOR) imposes rigor on the portrayal of the operational environment. TEFOR serves as an honest broker for the implementation of the OE in training threat emulators and capabilities development for test and evaluation, including Network Integration Evaluation (NIE) events.

The Army will conduct NIE 17.2 to further progress towards the completion of the Mission Command Network (MCN) 2020 Focused End State (FES) Objectives. The primary efforts of NIE 17.2 are the Programs of Record (PORs) designated as Systems Under Test (SUT) for Warfighter Information Network-Tactical (WIN-T) network. The Tri-Band Line of Sight (TRILOS) operational test will inform senior leaders on the operational effectiveness, suitability, and survivability of the new high bandwidth and WIN-T interoperable network radio. The TRILOS establishes a terrestrial link for a more robust network which significantly increases data throughput while reducing Size, Weight, and Power (SWP) requirements. The Tactical Communications Network-Lite/Network Operations and Security Center-Lite (TCN-L/NOSC-L) Follow On Test will inform senior leaders on the operational effectiveness, suitability, and survivability of the system on a High Mobility Multipurpose Wheeled Vehicle (HMMWV).

On or about 05 JUL – 09 AUG 2017, TRADOC / Joint Modernization Command (JMC), in coordination with Army Test and Evaluation Command (ATEC), Army Evaluation Center (AEC), Operational Test Command (OTC), & Systems of Systems Engineering and Integration Directorate (SOSE&I), will conduct a Live, Virtual, Constructive Force-on-Force exercise at Fort Bliss, TX and White Sands Missile Range (WSMR), NM (and other locations as necessary) to accomplish NIE 17.2 objectives.

The NIE 17.2 Endstate objectives are:

- Select potential Force Modernization concepts and capabilities assessed and demonstrated that assist in achieving integrated network capability for the Future Force.
- Validate that evaluated components, integrated with network, add operational value and do not increase complexity.
- Successful demonstration and assessment of concepts and capabilities that address selected FES and Army Warfighting Challenges (AWfCs).

1.1 Scope. TRADOC G-2 TEFOR requires technical and subject matter expertise (SME) support to assist in the replication of the OE threat portrayal and enable the Director,

TEFOR to certify the OE replication at NIE 17.2. TRADOC (JMC/ Army Capabilities Integration Center (ARCIC) Lead) in coordination with Headquarters, Department of the Army (HQDA) G-3/5/7, G-8, Chief Information Officers C-6, U.S. Army Forces Command, Assistant Secretary of the Army (Acquisition, Logistics and Technology) (ASA(ALT)), and ATEC will plan and conduct NIE 17.2 at Fort Bliss, TX, and WSMR from 05 JUL -09 Aug 2017 in order to inform key fielding decisions.

1.2 General Information

1.2.1 Period of Performance. The Period of Performance (POP) for the awarded contract will be: 05 Jul 17 – 09 Aug 17 (to allow time for analysis and final reporting).

1.2.2 Non-disclosure Requirements. All Contractor personnel (to include Subcontractors, teaming partners, and consultants) personally and substantially involved in the performance of this contract shall execute and submit a “Non-Disclosure Agreement for Contractor Employees” Form (See Attachment A). Execution of this Non-Disclosure Agreement for Contractor Employees (to include supervisors) is required prior to the commencement of any work on this contract and whenever replacement Contractor personnel are proposed. Any information obtained or provided in the performance of this contract shall only to be used in the performance of this contract. Additionally, the Contractor (and any Subcontractors, consultants or teaming partners) shall complete and sign Attachment B, Sensitive Data Non-Disclosure Agreement. Execution of Attachment B is required prior to the commencement of any work under this contract.

1.2.3 Hours of Operation. The work contained in this Performance Work Statement (PWS) may require Extended Work Week (EWW) hours (on an exception basis) and will be coordinated by the Program Manager and the Contracting Officer’s Representative (COR).

1.2.4 Privacy Requirements/Security.

1.2.4.1 Facility Clearance. Offerors on this contract must hold a Secret Facility Clearance as some of the work will be performed in Secret-level spaces at the JMC Simulation Center at Fort Bliss, TX.

1.2.4.2 Privacy Act. Contractors may have access to sensitive, privileged, or Privacy Act information. Personnel shall adhere to the Privacy Act, (5 U.S.C. § 552a) and applicable Agency rules and regulations. Contractor personnel shall not divulge or release privacy data or information developed or obtained in the performance of this contract award, until made public or specifically authorized by the Government. The Contractor shall not use, disclose, or reproduce a third-party company’s proprietary data, other than as authorized and required in the performance of this contract award. The Contractor shall notify the Primary COR within 24 hours, identifying personnel that no longer require access to Government information systems.

- 1.2.4.3 **Contractor Identification.** Each contractor employee shall be issued a badge that fully identifies the contractor employee. The Identification (ID) badge shall be made of nonmetallic material, easily readable and include employee's name, contractor's name, functional area of assignment and color photograph.
- 1.2.4.4 **Display of ID Badges.** Contractor personnel shall wear the ID badge at all times when performing work under this contract to include attending Government meetings and conferences. Unless otherwise specified in the contract, each contractor employee shall wear the ID badge in a conspicuous place on the front of exterior clothing and above the waist except when safety or health reasons prohibit such placement. The badge shall display, at a minimum, the employee's full name and legal name under which the Contractor is doing business. Contractor personnel shall wear badges at all times and shall identify themselves as Contractors at meetings, emails, telephone conversations, etc.
- 1.2.4.5 **Answering Phones.** Contractor personnel shall identify themselves as contractor employees when answering government phones.
- 1.2.4.6 **Utilizing Electronic Email.** When prime contractor or subcontractor personnel send email messages as part of the contract performance (or otherwise relating to contract matters), each sender shall include his/her name (both first and last names), e-mail address and the name of the individual's employer.
- 1.2.4.7 **Citizenship.** All contractor personnel assigned to this contract shall be U.S. citizens. The contractor shall provide employees that have a security clearance level of SECRET. The contractor shall comply with all appropriate Government security directives and regulations. In accordance with (IAW) Army Regulations and Air Force Instructions, all prospective contractors will undergo a verification process to determine the trustworthiness and suitability prior to being granted access to federal property. Limited access with escort may be granted (at the installation's discretion) for an interim period while investigations are being conducted. Security Managers, Trusted Agent or COR will submit all background investigations on prospective contractors requiring CAC and/or network access.
- 1.2.4.8 **Visit Requests.** Contractors must ensure an owning relationship is established in the Joint Personnel Adjudication System (JPAS) for each individual performing duty in support of this performance work statement/task order. Contractor Facility Security Officers (FSO) will send a Visit Request (VR) using JPAS for all contractors requiring access to facilities, classified information, access to information systems, and/or if required to maintain a clearance IAW the presiding contract. This will help ensure that employees are not denied entry to the installation.

1.2.4.9 **Government Issued Common Access Card CAC.** The common access card (CAC) is the Department of Defense (DoD) personal identity verification credential. In order to receive a CAC, every employee must be investigated as part of the Homeland Security Presidential Directive (HSPD-12 process. The type of investigation used in compliance with HSPD-12 adjudications is the National Agency Check with Inquiries. The National Agency Check with Law and Credit (NACLC) serves as the minimum type of investigation required to be issued a CAC. It consists of several elements, including database and local agency checks as well as written inquiries. The NACLC examines the last five years of an applicant's life, but no further back than the applicant's 18th birthday. The Contractor shall notify the Government when an employee departs so the card can be inactivated. The security manager and or trusted agent shall be responsible for retrieving the CAC from a departing contractor.

1.2.4.10 **AT Level I Training.** All contractor employees, to include subcontractor employees, requiring access to Army installations, facilities and controlled access areas shall complete AT Level I awareness training within 30 calendar days after contract start date or effective date of incorporation of this requirement into the contract, whichever is applicable. The contractor shall submit certificates of completion for each affected contractor employee and subcontractor employee, to the COR or to the contracting officer, if a COR is not assigned, within 10 calendar days after completion of training by all employees and subcontractor personnel. Anti-Terrorism (AT) level I awareness training is available at the following website:
<https://jkodirect.jten.mil>.

Army Regulation (AR) 25.2, Information Assurance, requires all personnel including contractors using Government computers or accessing Government networks, (NIPRnet or SIPRnet) to complete Information Assurance training. Contractor shall coordinate with COR to ensure training is conducted. CORs and the requiring activity will ensure that contractor personnel supporting Information Assurance (IA) functions are certified in accordance with DoD 8570.01-M. The COR and the requiring activity will ensure that all TRADOC contract instruments reflect this DoD requirement. As determined by the contracting officer, this certification requirement will be incorporated by reference and/or included in any performance work statement or statement of work. For existing contract instruments that lack this certification requirement, coordinate with the contracting officer to modify the contract in conjunction with the exercise of a contract option or as part of a separate contract modification action. Such contract action should occur as soon as is practicable.

Information Assurance Contractor Training and Certification (JAN 2008)

- (a) The Contractor shall ensure that personnel accessing information systems have the proper and current Information assurance certification to perform information assurance functions in accordance with (DoD) 8570.01-M,

Information Assurance Workforce Improvement Program. The Contractor shall meet the applicable information assurance Certification requirements, including

(1) DoD approved information assurance workforce certifications appropriate for each category and level as listed in the Current version of DoD 8570.01-M; and

(2) Appropriate operating system certification for information assurance technical positions as required by DoD 8570.01-M.

(b) Upon request by the Government, the Contractor shall provide documentation supporting the information assurance functions.

(c) Contractor personnel who do not have proper and current certifications shall be denied access to DoD information systems for the purpose of performing information assurance functions.

1.2.4.11 **iWATCH Training.** The contractor and all associated sub-contractors shall brief all employees on the local iWATCH program (training standards provided by the requiring activity Antiterrorism Officer (ATO)). This locally-developed training will be used to inform employees of the types of behavior to watch for and instruct employees to report suspicious activity to the COR. This training shall be completed within 30 calendar days of contract award and within 30 calendar days of new employees commencing performance with the results reported to the COR NLT 40 calendar days after contract award.

1.2.4.12 **Access and General Protection/Security Policy and Procedures.** The contractor and associated subcontractors' employees shall comply with applicable installation, facility, and area commander installation and facility access and local security policies and procedures. The contractor shall also provide all information required for background checks to meet installation access requirements to be accomplished by the installation Provost Marshal Office, Director of Emergency Services, or Security Office. The contractor workforce shall comply with all personal identity verification requirements as directed by DoD, HQDA, and/or local policy. In addition to the changes otherwise authorized by the changes clause of this contract, should the Force Protection Condition (FPCON) at any individual facility or installation changes, the Government may require changes in contractor security matters or processes.

1.2.4.13 **Operational Security (OPSEC) Awareness Training.** AR 530-2 Chapter 4 requires all Army personnel (including military, DA Civilians and contractors) to conduct initial OPSEC awareness training within 30 days of arrival at a new unit, and annual OPSEC awareness training every year after that. All Contractors must complete annual OPSEC Training requirements. The Contractor shall at all times adhere to installation OPSEC requirements such as installation entry/exit requirements, vehicle registration, on-base security restricted areas entry, etc. It is

the Contractor's responsibility to seek out and understand an installation's OPSEC requirements before initiating work for the first time at the installation.

1.2.5 Vehicle Registration. As required, the Contractor and Contractor personnel shall register their vehicles with the installation security forces office within 48 hours prior to reporting to their assigned job site.

1.2.6 Travel. Guidance for Contractor travel can be found in Federal Acquisition Regulation (FAR) 31.205-46, the General Services Administration Federal Travel Regulations (FTR), DoD Joint Travel Regulations (JTR) and Department of State Standardized Regulations (DSSR).

1.2.7 Travel Requests. The primary place of performance is Fort Bliss, TX. All requests for travel shall be submitted on SharePoint for review and approval by the COR prior to incurring cost, as travel will be reimbursed IAW the FTR, JTR, and/or DSSR. Contractors shall minimize the number of travelers and rental cars, and travel shall be scheduled during normal duty hours whenever possible. Requests for travel approval shall be prepared and processed through SharePoint, and shall include a description of proposed travel, a list of travelers, the contract number, Contract Line Item Number (CLIN), and be submitted at least 48 hours prior to travel for approval (see PWS para 6.1.8 and PWS Attachment C).

1.2.8 Data Rights. The Government shall have unlimited rights to all documents and materials produced under the Contract. **(No software is being produced under this contract.)** All written products produced shall be Government-owned and are the property of the Government with all rights and privileges of the ownership and copyright belonging exclusively to the Government. These products shall not be used or sold by the Contractor without prior written permission from the Contracting Officer.

SECTION C-2 ACRONYMS

2.0 Acronyms and Definitions. The following terms, as used throughout this Operational Environment/Core Functions PWS, have the meaning set forth below.

Acronyms	Definition
AEC	Army Evaluation Center
AKO	Army Knowledge Online
ARCIC	Army Capabilities Integration Center
ASA(ALT)	Assistant Secretary of the Army (Acquisition, Logistics and Technology)
ATEC	Army Test and Evaluation Command
ATGM	Anti-Tank Guided Missile
ATO	Antiterrorism Officer
AWfCs	Army Warfighting Challenges
JMC	Joint Modernization Command
C2	Command and Control
CDRLs	Contract Data Requirement Lists
CLIN	Contract Line Item Number
COR	Contracting Officers Representative
CPARS	Contractor Performance Assessment Reporting System
DAC	Department of Army Civilian
DFARS	Defense Federal Acquisition Regulation Supplement
DoD	Department of Defense
DoDD	Department of Defense Directive
ENDEX	End of Exercise
EWV	Extended Work Week
FAA	Federal Aviation Administration
FAR	Federal Acquisition Regulation <i>The principal set of rules established to govern the acquisition process of the Government purchasing goods and services.</i>
FES	Focused End State
FTR	Federal Travel Regulations <i>Prescribed by the General Services Administration for travel in the contiguous United States.</i>
G-2	Deputy Chief of Staff for Intelligence
GFP	Government Furnished Property
HMMWV	High Mobility Multipurpose Wheeled Vehicle
HQDA	Headquarters, Department of the Army
HSPD	Homeland Security Presidential Directive
IA	Information Assurance
IAW	In Accordance With
ISR	Intelligence Surveillance and Reconnaissance
JTR	Joint Travel Regulations <i>Prescribed by the DoD, for travel in Alaska, Hawaii, and outlying areas of the United States.</i>

KORNET	Russian Anti-Tank Guided Missile
MCN	Mission Command Network
NACLC	National Agency Check with Law and Credit
NIE	Network Integration Evaluation
NLT	No later than
OC	Observer Controller
OE	Operational Environment
OneSAF	One Semi-Automated Forces
OPFOR	Opposing Force(s)
OTC	Operational Test Command
POP	Period of Performance
POR	Program of Record
PRS	Performance Requirement Summary
PWS	Performance Work Statement <i>Explains concisely what is to be accomplished in terms of results so that the Government can monitor and evaluate the progress and final result of the project effectively.</i>
QA	Quality Assurance
QASP	Quality Assurance Surveillance Plan <i>Establishes performance standards and measures how the performance standards will be identified.</i>
QCP	Quality Control Plan
RPG	Rocket-Propelled Grenade
SME	Subject Matter Expert
SOSE&I	Systems of Systems Engineering and Integration Directorate
STAR	System Threat Assessment Report
SUT	System Under Test
SWP	Size, Weight and Power
TCN-L/NOSC-L	Tactical Communications Network-Lite/Network Operations and Security Center-Lite.
TEFOR	Threat Emulation Force
TRADOC	Training and Doctrine Command
TRILOS	Tri-Band Line of Sight
TTSP	Threat for Test Support Plan
UAS	Unmanned Aerial Surveillance
UAV	Unmanned Aerial Vehicle
U. S. C.	United States Code
WAWF	Wide Area Workflow <i>A web-based application that allows Contractors to electronically submit invoices and receiving reports and the Government to inspect, accept, receive, and pay electronically.</i>
WIN-T	Warfighter Information Network-Tactical

SECTION C-3 GOVERNMENT FURNISHED PROPERTY AND SERVICES

3.0 Government-Furnished Property (GFP) and Services. The Government will provide one Department of Army Civilian (DAC) to function as an Opposing Force(s) (OPFOR) Observer Controller (OC) to ensure appropriate Live OPFOR performance IAW established standards.

DRAFT

SECTION C- 4 CONTRACTOR-FURNISHED PROPERTY AND SERVICES

4.0 Contractor-Furnished Property and Services. The Contractor shall be responsible for providing management, labor, materials, equipment, and facilities, not otherwise provided as Government-furnished. The costs for contractor-furnished property must be included in the contractor's quoted proposal. No contractor-furnished property shall be separately charged to the Government except as specifically authorized/required by Government Contracting Officer/COR. At contract completion, the contractor shall remove all contractor-furnished property from Government facilities unless title has vested in the Government.

SECTION C-5 SERVICES REQUIRED

5.0 Services required. JMC is the exercise director for NIE 17.2. In support of the exercise director, the Director, TRADOC G-2 TEFOR provides oversight of the Red Team during the NIE. This PWS covers a requirement for contractor services provided by TEFOR-trained and certified red team personnel to make final coordination with JMC and to perform tasks under the direct guidance of the Director of TEFOR, required for the validation of Threat Emulation as appropriate to the OE. TEFOR requires contractor support to assist it with certifying the operational environment at NIE 17.2. Contractor personnel will be trained and certified to serve as red team personnel during the event¹. The Contractor shall perform the following services.

Task 5.1 Provide OPFOR Constructive Simulation Support for 24/7 operations.

5.1.1 Provide one OneSAF manager SME to provide command and control (C2) for OPFOR OneSAF Station Operators on-site at Fort Bliss.

5.1.2 Provide three OneSAF SMEs/operators to execute OPFOR operations in a constructive simulation environment on-site at Fort Bliss. These SMEs will be broken into three shifts of one operator over each 24-hour period. US Army will provide officer leadership and guidance to assist with constructive simulation management and execution.

Task 5.2 Provide Field Observers to monitor live OE replication.

5.2.1 Provide two field observer SMEs to record the threat and operational environment replication IAW Army regulations and TRADOC G-2 guidance.

Task 5.3 Operate and maintain the Unmanned Aerial Vehicles (UAVs).

5.3.1 Provide one 2-man C2 element to coordinate with Range Control, JMC G-3 Air Officer, and the Brigade Air Element; publish the contractor-provided OPFOR UAV operations plans for inclusion into the JMC-published Air Tasking Order; and coordinate UAV support requirements with the supported OPFOR unit. The team will provide 24-hour coverage (day-time/nighttime operations)

5.3.2. Provide three 3-man teams to fly and maintain 9 contractor-provided UAVs IAW Federal Aviation Administration (FAA) and Redstone Arsenal safety requirements: one operator (line-of-sight), one operator (manning control of the Intelligence, Surveillance,

¹ The OE is a forward-looking effort to more accurately discern the challenges the Army will face at the operational level of war and determine its inherent implications. The OE describes the composite conditions, circumstances, and influences that affect commanders' decisions on the employment of military capabilities. Analysis of the OE identifies potential implications for the U.S. Army training, experimentation, and doctrinal development communities; establishes the framework for thinking about threat capabilities and environmental influences on conflict; and identifies points of reference necessary for guiding the capabilities-based model for force development. (OE as defined in TP 71-20-3)

Reconnaissance (ISR) package), and one safety officer/emergency kill. The teams will provide 24-hour coverage (day-time/nighttime operations).

5.3.3. Unmanned Aerial Surveillance (UAS) Pilots to provide pre-scheduled flight time in support of OPFOR Units

5.4. Provide labor to support weapons-simulators employment for Live OPFOR Operations.

5.4.1 Provide two technical SMEs (weapons trainers/safety officers) to ensure the weapons simulators are integrated with OPFOR operations, and fully functioning.

5.4.2 Provide three threat emulators to operate the gas-powered weapons simulators defined in para 5.5.2.

5.4.3 Provide three drivers to operate the OPFOR Technical vehicles defined in para

Task 5.5 Provide Equipment for Live OPFOR Operations. Provide the following equipment. UAVs must have U.S. Army Airworthiness Release statements IAW Department of Defense Directive (DoDD) 5030.61 (DoD Air Worthiness Policy) for the provided aircraft to fly in the designated area of operations during NIE 17.2. Contractor must satisfy required safety releases of JMC and Fort Bliss TX prior to commencement of the event. Equipment support includes:

5.5.1 UAVs:

5.5.1.1 Provide three Group 1 UAS Fixed Wing with sensor package

5.5.1.2 Provide nine Group 1 UAS Rotary Wing with sensor package. Three rotary wing systems must have FLIR/thermal capability and be able to operate during limited visibility.

5.5.2 Other:

5.5.2.1 Provide two Rocket-Propelled Grenade-29 (RPG) gas-operated weapons simulators. The RPG-29 simulators must be capable of attaching and initiating the Multiple Integrated Laser Engagement System (MILES). The contractor must provide past performance which demonstrates successful MILES capability with the RPG-29 simulator.

5.5.2.2 Provide two (2) KORNET Anti-Tank Guided Missiles (ATGMs) gas operated weapons simulators. KORNET simulators must be capable of attaching MILES. The contractor must provide past performance which demonstrates successful MILES capability with the KORNET simulator.

5.5.2.3. Provide three (3) Technical vehicles with pedestal mounts to accept the KORNET ATGM and RPG-29.

5.5.2.4. Provide nine (9) Off-road Technical support vehicles for red teams in the field.

SECTION C-6 PROGRAM MANAGEMENT SUPPORT

6.0 Program Management Support. The Contractor shall provide complete program management support that shall fully integrate, manage, control, and document (in TRADOC G-2 SharePoint) all phases of the PWS requirements. All program reports and required documentation must be in the TRADOC G-2 SharePoint site and part of a program knowledge base that designated Government personnel can easily search and use for situational awareness and decision support.

6.1 Quality Control Plan (QCP). The Contractor shall submit a QCP within ten days after award of contract and update the QCP throughout contract POP. The QCP addresses methods for meeting performance standards delineated in section C-5, Specific Tasks. The basic principle of the QCP is that the Contractor is responsible for quality control and that the Contractor shall institute and maintain a capability to ensure the quality of the products and services required. The Contractor shall apply industry standards and best practices to develop a plan that describes the inspection system to cover services listed in the PWS including, at a minimum, the method of inspection, the specific areas to be inspected, frequency of inspections, the title and organization placement of the inspection and a baseline performance criteria for Contractor support. Quality Assurance (QA) practices in program management include, at a minimum, identification of quality control factors and processes, evaluation methods, process improvement, and risk management.

The Contractor shall maintain QCP compliance online in the TRADOC G-2 SharePoint repository that is accessible by designated Government personnel. The Government should be able to generate a monthly Quality Audit that references entries made in the Contractor's QCP compliance site.

6.1.2. Satisfaction Survey. The Contractor shall include in the QCP a satisfaction survey form. This form should also be online in SharePoint and allow designated Government personnel to complete the survey online. SharePoint workflow will send a link out to these personnel on a monthly basis to complete the surveys. Satisfaction survey results will become part of the program knowledge base accessible to the Government to identify trends and issues.

6.1.3. Problem Notification Report. The Contractor shall include in the QCP a plan to report problems or potential problems that affect performance under the contract to the COR within 24 hours. The report shall address, at a minimum, the nature and source of problem, Government action required, the impact on delivery schedules, corrective action(s) needed, and the anticipated increased Government costs. All Problem Notification Reports shall be incorporated into the Monthly Status Report (MSR) for the next reporting period. This form shall be online in SharePoint and have workflow to immediately notify the COR and other designated personnel of the incidence. The reports will become part of the program knowledge base accessible to the Government to identify trends and issues.

6.1.4. Customer Complaints. The Contractor shall include in the QCP procedures for responding to customer complaints. The Government will request customer feedback using the Customer Feedback Form in Attachment D. Upon receipt of a customer complaint, the COR will immediately forward the form to the Contractor. The Contractor shall address any complaints, contacting the submitter if necessary, and perform or re-perform the service within five workdays. The Contractor shall complete the appropriate portion of the form and submit to the COR for approval. The appropriate activity's COR will re-inspect the work within ten workdays, as applicable, and notify the Contractor of any deficiencies identified during the re-inspection. This form shall be online in SharePoint and have workflow to immediately notify the COR and other designated personnel of the incidence. The reports will become part of the program knowledge base accessible to the Government to identify trends and issues.

6.2 Resource Plan. The Contractor shall develop a project schedule, a plan to determine project resource estimates, and how to ensure all project costs are captured at event completion.

6.3 Travel

Travel shall be in accordance with the Joint Travel Regulation (JTR).

SECTION C-7 DELIVERY/ INSPECTION/ACCEPTANCE/INVOICING

7.0 Delivery, Inspection/Acceptance by the Government, and Invoicing.

Inspection and acceptance of all work performed, reports, and other deliverables will be performed by the Primary and Supporting CORs. The Primary COR monitors overall Contractor compliance with the PWS requirements and reports surveillance results to the Contracting Officer. The Supporting CORs perform the actual on-site contract surveillance for a specific activity and report surveillance results to the Primary COR. The COR for this requirement will be appointed in writing by the Contracting Officer prior to award.

7.1 Deliverables. All deliverables shall meet professional standards, as determined by the Government, in order to fulfill the requirements, set forth in this contractual documentation. All written deliverables are to be submitted for review and include a transmittal letter identifying the contract number. The Contractor shall be responsible for delivering all end items within the specified timeframes. The format for deliverables will be an agreed upon format between the Government and the Contractor, unless otherwise stated in this PWS. The Contractor shall utilize a secure electronic system to submit all invoices, such as Army Knowledge Online (AKO) or a SharePoint portal.

7.1.1 The Contractor shall work with the Director TEFOR to complete an operational environment/threat assessment matrix, informed by the Threat for Test Support Plan (TTSP) and the System Threat Assessment Report (STAR) documents for each system under test. This provides a methodology for OE/Threat validation.

7.1.2 Contractor shall provide a final written analysis of observations throughout the field and simulation event, No later than (NLT) 15 days of End of Exercise (ENDEX).

7.2 Contractor Performance Assessment.

The Government will evaluate the Contractor's performance IAW the Quality Assurance Surveillance Plan (QASP) prepared by the Government. The QASP establishes performance standards and measures, and how they will be identified. The QASP specifies what will be measured, the frequency of the surveillance, and the acceptable level of performance.

All deliverables will be inspected by the Government for content, completeness, accuracy, and conformance to contract requirements. Inspection will include validation of information as specified in the contract.

7.2.1 Basis of Inspection and Acceptance. The basis for inspection and acceptance will be Contractor compliance with the requirements as set forth in the contract award, the Contractor's response and other terms and conditions of the contract including the Government QASP. Any products and services rejected shall be corrected IAW the applicable clauses.

- i. Reports, documents, and narrative type deliverables will be accepted when all discrepancies, errors or other deficiencies identified by the Government have been corrected.
- ii. The Contractor shall use best commercial practice for formatting deliverables.
- iii. All the Government's comments to deliverables shall either be incorporated in the succeeding version or the Contractor must demonstrate to the Government's satisfaction why such comments should not be incorporated.
- iv. If the Government finds that a deliverable contains spelling errors, grammatical errors, improper format, or otherwise does not conform to the requirements stated, the document may be immediately rejected without further review and returned to the Contractor for correction and re-submission.

7.3 Invoice Submission. The Contractor shall use Wide Area Workflow (WAWF) to submit monthly invoices IAW Defense Federal Acquisition Regulation Supplement (DFARS) 252.232-7003. WAWF is a web-based application that allows Contractors to electronically submit invoices and receive reports and allows the Government to inspect, accept, receive, and pay electronically. The Contractor shall create invoices through WAWF website using prompts to input required information.

7.3.1 Invoices for Travel CLINs. The following applies to submission of invoices for payment of travel. The Contractor may invoice monthly on the basis of cost incurred for travel CLINs. The invoice shall include the period covered by the invoice, the CLIN number, and name. For travel costs, invoices shall reflect the Contractor's actual expense for the item, plus General and Administrative costs. These charges shall not exceed limits specified in the contract award. No charges will be paid by the Government which are not specifically detailed in this contract.

In addition, the Contractor shall provide the Government the following detailed information for each invoice submitted, as applicable. Separate forms (in SharePoint), shall be submitted for travel with separate columns for the following:

7.3.1.1 Project Total Travel. This will identify all current and past travel on the project and their total project costs billed. The listing shall include separate columns and totals for the following information concerning the current invoice period and the project to date:

- i. Current invoice period.
- ii. Names of persons traveling.
- iii. Number of travel days.
- iv. Dates of travel.
- v. Number of days per diem charged.
- vi. Per Diem rate used.
- vii. Total per diem charged.
- viii. Transportation costs.
- ix. Other charges.
- x. Total charges.

7.3.1.2 CLIN/Task Total Travel. This will identify all current and past travel on the project and their total CLIN/Task costs billed. The listing shall include separate columns and totals for the current invoice period and the project to date:

- i. Current invoice period.
- ii. Names of persons traveling.
- iii. Number of travel days.
- iv. Dates of travel.
- v. Number of days per diem charged.
- vi. Per Diem rate used.
- vii. Total per diem charged.
- viii. Transportation costs.
- ix. Total charges.

SECTION C-8 TECHNICAL EXHIBITS

8.0 Technical Exhibits. - None

DRAFT

Section C-9 - CONTRACT DATA REQUIREMENTS LIST (CDRLs)

<u>DELIVERABLE</u>	<u>FREQUENCY</u>	<u>MEDIUM/FORMAT</u>	<u>SUBMIT TO</u>
Quality Control Plan (QCP). PWS para.6.1	Initial due within 10 days after contract award and updated throughout contract performance.	Electronic format	KO and COR
Satisfaction Survey PWS para. 6.1.2	Provide with QCP	Electronic format	COR
Problem Notification Report PWS para. 6.1.3	Provide with QCP and provide within 24 hours of problem or potential problem.	Electronic format	COR
Customer Complaints. PWS para.6.1.4	Provide procedures in the QCP. Contractors shall respond to all customer complaints.	Customer Feedback Form (Attachment D)	COR
Resource Plan (project schedule) PWS para. 6.2	Estimates due by the 5 th workday after Government notification and actual amounts due by 5 th workday after project completion	Electronic	COR
Invoice Submission PWS para.7.3	Monthly	Electronic format.	Wide Area Workflow

SECTION C-10 ATTACHMENTS AND FORMS

Attachment A	Non-Disclosure Agreement for Contractor Employees
Attachment B	Sensitive Data Non-Disclosure Agreement
Attachment C	Travel Authorization Request Form
Attachment D	Customer Feedback Form
Attachment E	Performance Requirement Summary (PRS)

ATTACHMENT A

Non-Disclosure Agreement for Contractor Employees

1. I, **INSERT NAME** , an employee of **INSERT COMPANY NAME** , understand as part of my duties as an employee working under contract number **INSERT CONTRACT NUMBER** that I may acquire or have access to privileged, proprietary, or otherwise sensitive information. This access may include direct access to the information that is specifically provided to me for work under the Contract or indirect access to information incidental to the work performed under the Contract.
2. It is the United States Government's intent to strictly protect and manage access to, and to prevent unauthorized disclosure of the Government's information. This includes preventing disclosure of sensitive and non-public information to anyone not working on the Contract.
3. Protected Information may include, but is not limited to: proprietary information; advance procurement information; source selection information; trade secrets; internal Government operational information; and confidential business information submitted by a Contractor regardless of whether such information is written, oral, or designated as sensitive, proprietary, or confidential at the time of its disclosure.
4. I certify that I shall not use Protected Information other than in performance of my assignment under the Contract, and that I shall only disclose Protected Information to either **INSERT COMPANY NAME** employees working on this Contract, Government employees, or other personnel authorized by the OE/CORE Program Manager or the Contracting Officer's Representative (COR).
5. I further acknowledge that the unauthorized disclosure of Protected Information to anyone not associated with the support of the contract could result in a personal and/or organization conflict of interest for myself and/or **INSERT COMPANY NAME** .
6. I understand and agree that access to Protected Information precludes me from participating, on my own behalf, on behalf of **INSERT COMPANY NAME** or subsequent employers, or on behalf of others in the preparation of cost or technical proposals or taking part in contract negotiations involving or related to future requirements or project, if such participating involves utilization of Protected Information.
7. I agree that I will clearly identify myself as a representative of **INSERT COMPANY NAME** prior to engaging in any communications through which Protected Information may be obtained from Government personnel or third parties (e.g., meetings, telephones, and other situations where Contractor status is not obvious.)

8. I will not disclose or use any sensitive and non-public information or any Protected Information in any manner inconsistent with the laws, regulations, or policies of the United States Government or any agency thereof, including 18 U.S.C. § 1905, Disclosure of Confidential Information, and 41 U.S.C. § 2102, Prohibitions on Disclosing and Obtaining Procurement Information.

9. I shall take all reasonable precautions to prevent the disclosure of Protected Information to any unauthorized party. I shall report to the OE/CORE Program Manager any violation of this Agreement. If I become aware of any improper release or disclosure of Protected Information by another party, I shall report this to the OE/CORE Program Manager and the Contracting Officer's Representative or the Contracting Officer, in writing, immediately.

10. I further understand that the penalty for unauthorized disclosure or use of Protected Information may result in disciplinary actions up to and including dismissal from my employer.

Employee Name (Printed)

Employee Signature

Date

Employer/Supervisor Name (Printed)

Employer/Supervisor Signature

Date

INSERT COMPANY NAME
INSERT COMPANY ADDRESS

ATTACHMENT B

SENSITIVE DATA NON-DISCLOSURE AGREEMENT

Department of the Army, U.S. Army Training and Doctrine Command (TRADOC) G-2

SENSITIVE DATA NON-DISCLOSURE AGREEMENT

AN AGREEMENT BETWEEN [INSERT NAME OF CONTRACTOR],
AND THE UNITED STATES

1. [INSERT NAME OF CONTRACTOR] hereby accepts the obligations contained in this agreement in consideration of [INSERT NAME OF CONTRACTOR] being granted access to sensitive data. As used in this Agreement, sensitive data is marked or unmarked "sensitive but unclassified information", including oral communications, that meets the standards set by OMB A-130 and is otherwise identified as such by the TRADOC G-2. [INSERT NAME OF CONTRACTOR] understands any data or systems of records protected from unauthorized disclosure by the provisions of Title 5, United States Code Sections 552 (often referred to as ("The Freedom of Information Act") and 552a ("The Privacy Act") is/are sensitive data. In addition, other categories of information, including but not limited to medical, personnel, financial, investigatory, visa, law enforcement or other information which, if released, could result in harm or unfair treatment to any individual or group, or could have a negative impact upon individual privacy, Federal programs, or foreign relations is sensitive data. The term includes data for which the improper use or disclosure could adversely affect the ability of the United States Army and/or TRADOC G-2 to accomplish its mission, as well as proprietary data and information received through privileged sources. [INSERT NAME OF CONTRACTOR] understands and accepts that by being granted access to sensitive data, special confidence and trust has been placed in it by the United States Government.

2. [INSERT NAME OF CONTRACTOR] acknowledges that it has been given access to TRADOC G-2 sensitive data/information to facilitate the performance of duties assigned to it for compensation. [INSET NAME OF CONTRACTOR] understands its responsibility to safeguard sensitive data disclosed to it and to refrain from disclosure sensitive data to persons not requiring access for performance of official duties. Before disclosing sensitive data, [INSERT NAME OF CONTRACTOR] must consult with the Contracting Officer's Representative (COR).

3. [INSERT NAME OF CONTRACTOR] has been advised that any breach of this Agreement may result in the termination of its access to sensitive data, which, if such termination effectively negates [INSERT NAME OF CONTRACTOR's] ability to perform assigned duties, may lead to the termination of this Contract and/or other relationships with the Departments or Agencies that granted it access. [INSERT NAME OF CONTRACTOR] is aware that unauthorized release or mishandling of sensitive data/information may be grounds for adverse action against [INSERT NAME OF CONTRACTOR]. Unauthorized disclosure and/or misuse of Privacy Act data/information

or other sensitive data/information may constitute a violation of United States civil and criminal law.

4. [INSERT NAME OF CONTRACTOR] understands that all sensitive data/information to which [INSERT NAME OF CONTRACTOR] has access or may obtain access by signing this Agreement is now and will remain the property of, or under the control of the United States Government. [INSERT NAME OF CONTRACTOR] agrees that it must return all sensitive data/information which has, or may come into its possession or for which it is responsible because of such access:

- (a) upon demand by an authorized representative of the United States Government; or upon the conclusion of the contract or other relationship with the Department or Agency that last
- (b) granted me access to sensitive data; or
- (c) upon the conclusion of the contract or other relationship that requires access to sensitive data.

Unless and until [INSERT NAME OF CONTRACTOR] is released in writing by the cognizant Contracting Officer or his/her authorized representative, [INSERT NAME OF CONTRACTOR] understands that all conditions and obligations imposed upon it by this Agreement apply during the time [INSERT NAME OF CONTRACTOR] is granted access to sensitive data/information and at all times thereafter.

5. [INSERT NAME OF CONTRACTOR] further agrees to the below terms.

(a) Signed Agreements. The Contractor agrees to sign an agreement to this effect with carriers, and other private or public entities providing proprietary data for performance under this Contract. As part of this Agreement, the Contractor shall inform all parties of its agreement to allow certain Government-designated Contractors' access to all data/information. One copy of each signed agreement shall be forwarded to the Contracting Officer.

(b) Government Designated Contractors. The Contractor agrees to allow the below listed Government-designated support Contractors, possessing appropriate proprietary agreements and retained by the Government to advise the Government on cost, schedule and technical matters pertaining to this acquisition, access to any unlimited rights data acquired under the terms and conditions of this contract and to sign reciprocal non-disclosure agreements with them. One copy of each signed agreement shall be forwarded to the Contracting Officer.

List designated Contractors:

All Government-designated Contractors stated herein, or added at a future date shall also enter into non-disclosure agreements with all parties providing proprietary information to the Contractor.

- (b) Remedy for Breach. The Contractor acknowledges that any breach or violation of the Agreement shall constitute a material and substantial breach of the terms, conditions and provisions of the Contract and that the Government may, in addition to any other remedy available, terminate this contract for default IAW the provisions of FAR 52.249-8 Default (Fixed-Price Supply and Service). Nothing in this Agreement or Contract shall be construed to mean that the Government shall be liable to the owners of proprietary information in any way for the unauthorized release or use of proprietary information by this Contractor or its Subcontractors.

**GOVERNMENT
WITNESS**

**CONTRACTOR
ACCEPTANCE**

THE EXECUTION OF THIS AGREEMENT WAS
WITNESSED BY THE UNDERSIGNED.

[INSERT NAME OF CONTRACTOR]

BEFORE ACCESSING SENSITIVE DATA OF THE UNITED STATES GOVERNMENT.

SIGNATURE

SIGNATURE

DATE

DATE

TITLE/POSITION:

TITLE/POSITION:

ATTACHMENT C

TRAVEL AUTHORIZATION REQUEST FORM

Travel Authorization Request Form														
Travel Request No#:														
Date of Request:														
Order/CLIN Travel Supports:														
Effort:														
Company:														
Remarks/Explanations (weekend travel, Federal holiday travel, etc. include any associated benefit to government):														
Name of Traveler		Trip Locations		Estimated Travel Date(s)		Trip	Government Officer	Estimated	Estimated	Estimated	Estimated	Other	Description of Other	
First	Last	From	To	mm/dd/yy	mm/dd/yy	Description/Purpose	Requesting Travel	Airfare	Lodging	M&IE	Rental Car	Travel \$\$	Expenses	Total
														\$0.00
														\$0.00
*We certify all travel costs are accordance with the FTR, JTR, and/or DSSR.														
Total Estimated Travel for this Request:													\$0.00	
Total Estimated Remaining Before Request:													\$0.00	
Total Estimated Remaining After Request:													\$0.00	

ATTACHMENT D
CUSTOMER FEEDBACK FORM

Date/Time of Service: _____

Feedback Originator/Telephone #: _____

Service(s) Received/Requested: _____

1.) Overall, how would you rate the quality of the service(s)?

5	4	3	2	1
Exceptional	Very Good	Satisfactory	Marginal	Unsatisfactory
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

2.) Nature of complaint or comment:

3.) What is one thing the Contractor could do to improve your level of satisfaction?

Thank you for taking time to assist us in improving the level of service.

XX

Remainder of form is for use by the Contractor/COR:

Date/Time Contractor Received Feedback _____ Contract: _____

Contractor Determination/Explanation: Complaint Valid ☐ Complaint Not Valid ☐

(CONTINUE ON REVERSE)

Action Taken by Contractor:

(CONTINUE ON REVERSE)

Contractor Signature: _____ Date: _____

COR Determination: Complaint Valid ☐ Complaint Not Valid ☐

Corrective Action Sat ☐ Corrective Action Unsat ☐

COR Signature: _____ Date: _____

ATTACHMENT E

Performance Requirement Summary (PRS)

Performance Requirement	Method of Measurement	Acceptable Quality Level (AQL)	Performance Incentive/Disincentive	PWS Reference
Provide OPFOR Constructive Simulation Support for 24/7 operations	Inspection by the COR and Customer feedback	Timeliness: 95% of SME requests are completed by the required timelines or by coordinated extension. Quality: Meets criteria of inquiries and requests. Acceptable to allow rework of minor discrepancies within 1 workday.	When performance is below standard for a given time period, require the contractor to re-perform the service at no additional cost to the Government.	5.1
Provide Field Observers to monitor live OE replication	Inspection by the COR and Customer feedback	Timeliness: Field observers are in place 95% of the time. Quality: Meets criteria of inquiries and requests. Acceptable to allow rework of minor discrepancies within 1 workday.	When performance is below standard for a given time period, require the contractor to re-perform the service at no additional cost to the government.	5.2
Operate and maintain the Unmanned Aerial Vehicles (UAVs)	Inspection by the COR and Customer feedback	Timeliness: At least 95% of SME/Operators are coordinated for onsite support at Fort Bliss. Changes are coordinated with the Government for extensions or exceptions. Quality: Meets criteria of inquiries and requests. Acceptable to allow rework of minor discrepancies within 1 workday.	When performance is below standard for a given time period, require the contractor to re-perform the service at no additional cost to the government.	5.3.
Provide labor to support weapons-simulators employment for Live OPFOR Operations	Inspection by the COR and Customer feedback	Timeliness: At least 95% of observer SME's are available to validate threat and the OE. All others are coordinated with the Government for extensions or exceptions. Quality: Meets criteria of inquiries and requests. Acceptable to allow rework of minor discrepancies within 1 workday.	When performance is below standard for a given time period, require the contractor to re-perform the service at no additional cost to the government.	5.4.
Provide Equipment for Live OPFOR Operations	Inspection by the COR and Customer Complaints	Timeliness: – At least 95% of all labor to maintain UAV's and support deployment will be available for the training events. All others are coordinated with the Government for extensions or exceptions. Quality: Meets criteria of inquiries and requests. Acceptable to allow rework of minor discrepancies within 1 workday.	When performance is below standard for a given time period, require the contractor to re-perform the service at no additional cost to the government. Document past-	5.5